

MAR 19 2007

Appln. No. 10/624,857
Amendment dated March 19, 2007
Reply to Office Action mailed December 18, 2006

REMARKS

Reconsideration is respectfully requested.

Claims 1 through 20 remain in this application. No claims have been cancelled or withdrawn. Claims 23 through 25 have been added.

The Examiner's rejections will be considered in the order of their occurrence in the Office Action.

Paragraph 2 of the Office Action

Claims 1 through 22 have been rejected under 35 U.S.C. Section 103(a) as being unpatentable over DRM (<http://www.reed-electronics.com/semiconductor/article/CA231640>).

Claim 1 requires "receiving a diagnostic code for a component of a computer system" and "generating an authentication code *associated with* the diagnostic code" (emphasis added) .

In the rejection of the Office Action, it is contended that:

DRM teaches...

generating an authentication ... associated with the diagnostic code (section "DRM enterprise server", subsection "authentication", i.e., the user privilege is associated with the authentication for authorization, thereby the e-diagnostic is associated with the authorization)."

It is then conceded that:

These passages of DRM do not explicitly mention "code" in the sense of the claim.

However, it is submitted that the DRM document lacks more than simply mentioning "'code' in the sense of the claims", as the claim language clearly requires "generating an authentication code *associated with* the diagnostic code", and the referenced portion of the DRM document clearly discusses authentication of a *user*, and not any authentication of any diagnostic code

Appln. No. 10/624,857
Amendment dated March 19, 2007
Reply to Office Action mailed December 18, 2006

Looking to the portion of the DRM document in more detail, it states
(emphasis added):

• Authentication: When a user logs in to the DRM system via the DRM enterprise server, he is authenticated against an LDAP (Lightweight Directory Access Protocol) server. Typically, a login page prompts for a username and password. LDAP is the tool of choice for managing users because it has many sophisticated levels of user management. It also has become dominant as a standard for user management with enterprise systems, allowing all of a company's users to be managed in one central place for all of its internal systems. The DRM enterprise server builds on the LDAP foundation to enhance security as users relate to tools and privileges.

However, it is clear that the discussion here is directed to the authentication of the users of the system, and not to any diagnostic code. It is submitted that one of ordinary skill in the art, considering this portion of the DRM document, would understand that it is the user, and not any element of the system or particularly any diagnostic code, that is being "authenticated" here. It is not understood exactly how "the user privilege is associated with the authentication for authorization" and "thereby the e-diagnostic is associated with the authorization" relates to this, as there is nothing in the text of the DRM document that states or suggests that there is any connection with a user being "authenticated" with any diagnostic code being "authenticated", as there is no suggestion that only "authenticated" users have anything to do with diagnostic codes. One of ordinary skill in the art recognizes that the fact that a user must be authorized to access a system does not authenticate any diagnostic codes. The DRM document does not suggest any such connection between an authorized user and an authenticated diagnostic. There is no suggestion that the "authenticated" user has anything to do with the reception or generation of diagnostic codes. There is also no mention of any association of this user "authentication" with any diagnostic code that is received, or that the authentication of a user has any connection to a diagnostic code, or the legitimacy of the diagnostic code.

Appln. No. 10/624,857

Amendment dated March 19, 2007

Reply to Office Action mailed December 18, 2006

Further, it is noted that the DRM document states:

- Authorization: The DRM system manages the privileges of users and groups. These users and groups are defined in LDAP. For each group, the DRM system has a set of privileges set up by the administrator. There are some built-in privileges, and the DRM system can be extended to support any number of custom privileges. These typically control access to parts of the application as well as what can be done within the application, such as creating or deleting monitoring rules, or viewing ARAMS data. When a user logs in to the DRM system, privileges are granted based on group membership.

Again, this portion of the DRM document simply addresses the legitimacy of the user, and has nothing to do with the authenticity or authentication of a diagnostic code that is received.

And it is further asserted in the rejection of the Office Action that:

Nevertheless, it was well known in the art to have a "code" for the motivation of having a physical software program for actuating the authentication algorithm (the algorithm used in the code).

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to modify DRM for the motivation noted in the previous paragraphs so as to teach the claimed invention.

It is not understood what having "a 'code' for the motivation of having a physical software program for actuating the authentication algorithm" means, as it is not understood, for example, the meaning of a "physical software program". In any event, the assertion that this is "well known" is traversed and the Examiner is asked to explain what this means and to show evidence that this is indeed "well known" in the art.

The rejection further states:

Regarding claim 2 (authentication code using date value, etc.), such particular features are well known in the art for the purpose of security and for the purpose of keeping track of data.

Regarding claim 3 (authentication code using serial number, etc.), such particular features are well known in the art for the purpose of security and for the purpose of keeping track of data.

Appln. No. 10/624,857
Amendment dated March 19, 2007
Reply to Office Action mailed December 18, 2006

Again, it is submitted that the DRM document does not disclose an "authentication code" according to the requirements of claim 1, and therefore it is submitted that the DRM document does not disclose it, and the allegedly "well known" character of these modifications of the code is traversed. The Examiner is respectfully requested to provide evidence of the alleged "well known" nature of authentication codes including dates and serial numbers.

Also, assuming for the purposes of argument only that the suggestion in the rejection that the username and password scheme of the DRM document discloses the claimed authentication, it is submitted that this would lead one of ordinary skill in the art away from the use or inclusion of any date or serial number in the authentication code, as one of ordinary skill in the art recognizes that a username and password does not include these elements.

The rejection of claims 4 through states:

Regarding claims 4-8, such particular features are well known in the art for the purpose of security.

Even if one assumes for the purposes of argument only that such "features are well known for the purpose of security", it is submitted that this would not motivate one of ordinary skill in the art to integrate these elements in an authentication code associated with a diagnostic code, as there is nothing in the DRM document that suggests that security (beyond simply logging in with a password) is needed.

MAR 19 2007

Appln. No. 10/624,857
Amendment dated March 19, 2007
Reply to Office Action mailed December 18, 2006

Withdrawal of the §103(a) rejection of claims 1 through 22 is
therefore respectfully requested.

CONCLUSION

In light of the foregoing amendments and remarks, early
reconsideration and allowance of this application are most courteously
solicited.

Respectfully submitted,

WOODS, FULLER, SHULTZ & SMITH P.C.



Date:



Jeffrey A. Proehl (Reg. No. 35,987)
Customer No. **40,158**
P.O. Box 5027
Sioux Falls, SD 57117-5027
(605)336-3890 FAX (605)339-3357